UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/607,430	06/27/2000	Guangyu Zhao	CISCO-2402	7891

7590 07/12/2005

Jonathan Velasco
Sierra Patent Group, Ltd.
P.O. Box 6149
Stateline, NV 89449

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/607,430	ZHAO ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *RCE filed on 05/31/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-27 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-27 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/31/2005 has been entered.

2. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. Claims 1-27 are pending.

Response to Arguments

5. Applicant's arguments filed 05/31/2005 have been fully considered but they are not persuasive.

- Examiner has fully considered Applicant's interpretation of Chen et al (5,832,208 A) teaching (page 8 and 9 of the response).

- As per Applicant's arguments requesting Examiner answers the questions raised by applicant, Examiner makes the following remarks:

1) with respect to the question number 1, examiner refers Applicant to the facts that Chen clearly and explicitly disclose the term "e-mail message" is used **for convenience** and it is used to describe all types of files, including messages, broadcasts and communications used within, sent from or received by a mail server. **It also disclose agent 110 do intercept and scan all incoming files** in order to give virus protection (see col.6, lines 54-63). Therefore Applicant's perception of an example of e-mail system of Chen and ignoring the other options presented by chen do not expedite the process of prosecution.

2) with respect to question number 2, examiner makes the following remarks:
The features upon which applicant relies (i.e.**" scanning all of the emails in an email system"**,) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Therefor the question of where and why (question number 3) scanning is being done is irrelevant to claim language. The claim language disclose intercept of incoming files, Chen disclose the e-mails are only an example and it is used to describe all types of files, including messages, broadcasts and communications used within, sent from or received by a mail server. **It also disclose agent 110 do**

intercept and scan all incoming files in order to give virus protection (see col.6, lines 54-63).

- As per Applicant's arguments that "Chen does not teach, disclose, nor otherwise suggest performing virus protection until after message somehow associated with an application program ("generated within, sent from, or received by the Lotus Notes program.")" see page 10, lines 11-14 of the response excluding the spaces between the lines, Examiner refers Applicant to the following remarks:

a) Chen et al does disclose performing virus protection to incoming files regardless of their association with an application or not (see col.6, lines 54-63 where the Lotus note program Applicant refers to is used only as an example, the other example given is database programs that allows for attachments, However Chen clearly and explicitly disclose the term "e-mail message" is used for convenience and it is used to describe all types of files, including messages, broadcasts and communications used within, sent from or received by a mail server. It also disclose agent 110 do intercept and scan all incoming files in order to give virus protection.

b) Applicant's above arguments implies that Applicant's invention differs from Chen by giving protection to files without any association with an application program. However step b of claims 1, 10, 16 and 22 of Applicant's invention clearly disclose association of intercepted files with anti-virus application before they are transferred to a file system by subjecting the incoming files to virus detection and removal.

Therefore Applicant's arguments are in contrast with limitations set forth in the above claims and where such limitations are disclosed by Chen as described in "a)" above.

C) Examiner refers Applicant to the meaning of the application program (application program is a computer software program designed for specific job such as word processing, accounting, spreadsheet, etc, please see any computer dictionary such as Microsoft dictionary or Newton's telecom dictionary). Therefore it is clear from the above definition, that any file created has an association with a computer software program and therefore transmission of such a file, interception and receipt has such an association based on the above definition.

Therefore Applicant's arguments with respect to "Chen does not teach, disclose, nor otherwise suggest performing virus protection until after message somehow associated with an application program ("generated within, sent from, or received by the Lotus Notes program.")" are not persuasive since Chen do disclose such a protection as described above.

- As per applicant's arguments with respect to independent claims 1, 10, 16 and 22 that Chen et al do not disclose "intercepting incoming files before they reach a file system" page 10 line 1 of the response; and "intercepting incoming files before they are transferred to a file system" page 11, lines 12-13 of the response

excluding spaces between the lines, examiner refers applicant to the following remarks:

d) in order to emphasize why Chen et al disclose the above limitations examiner break the above limitation into two phrases in order to simplify the arguments.

1) The phrase « intercepting incoming files » clearly indicate that action of interception is being done on incoming files, therefore the question is when Chen do disclose the act of interception on incoming files. Applicant's arguments on page 9, last paragraph, page 10, lines 1-14 implies that Applicant agrees that act of interception is being done by agent 110 but disagrees of when such act is being done. That's why Applicant has highlighted the phrase "**before**" to emphasize on the timing of the interception and not the act itself. Therefore Chen do disclose the act of interception of files as demonstrated on col.6, lines 54-58 where all types of files, messages, broadcasts and communications are being scanned by agent 110; or col.7, lines 32-35 where agent 110 monitors files for any type of attachments; agent 110 corresponds to Applicant's interceptor as interpreted by examiner in the last office action.

2) The question of timing of when the interception is being done is disputed by Applicant, where Applicant argues that Chen do not disclose interception of files before they reach a file system (emphasized added).

Examiner refers Applicant to Chen et al. col.6, lines 58-63 where "e-mail messages" is being used to describe all types of files, messages, broadcasts and communications used within, sent from or received by a mail server. Therefore Examiner considers any reference to e-mail messages corresponds to incoming files of Applicant's claims limitations. As an example" scanning of all e-mail messages corresponds to scanning of all incoming files as it was recited in the non-final office action.

Chen et al. col.5, lines 54-56 refer to centralized virus detection operations at the server level. Therefore Examiner considers any reference to e-mail server or other name server by Chen et al corresponds to "networked server" of Applicant's claim limitation as it was recited in the non-final office action.

Applicant's claim language state interception before files are transferred to **a file system** of the server. Chen et al disclose on col.6, lines 54-61 and fig.2 interception of files sent to mail server by agent 110

Chen et al abstract disclose interception of files for virus detection before being transferred to the message system (file system). Chen discloses "the agent is located at the server computer and provide **an interface** between the anti-virus module and the message system". Therefore any message received by the server is subjected to virus detection by the agent 110 and then be received by the message system or file system.

- **Examiner, however would reconsider if Applicant's claim language disclose the specific differences of the timing of the interception more clearly (example: interception takes place before the message received by the server and not the file system within the file server; or interception is being done within a firewall, etc..). However such clarity should have support in the specification.**

Claim Rejections - 35 USC § 102

1. **Claims 1-5, 10-13, 16-19 and 22-25** are rejected under 35 U.S.C. 102(b) as being anticipated by Chen et al (5,832,208 A).

Examiner refers Applicant to col.6, lines 58-63 where "e-mail messages" is being used to describe all types of files, messages, broadcasts and communications used within, sent from or received by a mail server. Therefore Examiner considers any reference to e-mail messages corresponds to incoming files of Applicant's claims limitations. As an example" scanning of all e-mail messages corresponds to scanning of all incoming files.

Col.5, lines 54-56 refer to centralized virus detection operations at the server level. Therefore Examiner considers any reference to e-mail server or other name server by Chen et al corresponds to "networked server" of Applicant's claim limitation.

Col.6, lines 1-4 disclose that the system is capable of scanning all incoming files as they are received.

As per claim 1 Chen et al (5,832,208 A) teach in a networked server (see fig.2, item 130 where the mail server corresponds to networked server) having a file system therein (see fig.2, item 140; col.7, lines 11-16 where the message system corresponds to applicant's file system), a virus detection monitoring system (see abstract where detection and removal of virus application in combination with server network and peripheral devices and interfaces corresponds to Applicant's virus detection monitoring system that monitors incoming files for virus) comprising:

a) a check-in interceptor configured to monitor the network server for incoming files and intercept incoming files before said files are transferred to the file system of the server (see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed) and

b) an anti-virus interface operatively coupled to said check-in interceptor (see fig.2, item 110 where item 110 also corresponds to Applicant's anti-virus interface, that is the agent not only monitors the incoming files as an check in interceptor but it also act as an interface between the server and the antiviral application of 120; also see col.7, lines 48-56 where upon detection of attachment it send the file to anti virus application), said anti-virus interface configured to transfer the incoming files, which are intercepted, to an anti-virus application for virus detection and removal (see col.7, lines 48-67 where if virus detected then the infected attachment is being deleted).

As per claim 2 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 1 wherein said anti-virus interface is further configured to receive from said anti-virus application a signal indicating whether a virus was detected in the intercepted incoming file and whether the virus was removed (see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5) .

As per claim 3 Chen et al (5,832,208 A) Chen et al teach the virus detection monitoring system of claim 1, wherein said check-in interceptor is further configured to prevent an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file (see fig.2, item 110 where the agent

corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed and that represent the act of prevention).

As per claim 4 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 1, wherein said check-in interceptor is further configured to prevent an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application (see col.8, lines 7-15 where if the attachment or virus is not removed after the interception as outlined in claim 1 above, then attempt to cure the file being conducted and only in case of file repaired that the agent may attachment may be re-attach to the file by the agent which means that if not cured or not removed the incoming file will not be forwarded by the agent).

As per claim 5 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 1 wherein said anti-virus interface is further configured to receive from said anti-virus application a signal indicating whether a virus was detected in the intercepted incoming file (see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5), said check-in

interceptor further configured to communicate the signal to a user submitting the intercepted incoming file (see col.7, lines 60-65 where the alert may be transmitted to network node originated the infected attachment that corresponds to the user who submitted the virus in the first place).

As per claim 10 Chen et al (5,832,208 A) teach in a networked server (see fig.2, item 130 where the mail server corresponds to networked server) having a file system (see fig.2, item 140; col.7, lines 11-16 where the message system corresponds to applicant's file system) therein, a method for virus detection monitoring (see abstract where detection and removal of virus application in combination with server network and peripheral devices and interfaces corresponds to Applicant's virus detection monitoring system that monitors incoming files for virus) comprising:

a) intercepting incoming files before the incoming files are transferred to the file system of the server (see fig.2, item 110 where the agent intercepts and check all incoming files; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed); and

b) transferring the incoming files which are intercepted to an anti-virus application for virus detection and removal (see col.7, lines 48-67 where if virus detected then the infected attachment is being deleted).

As per claim 11 Chen et al (5,832,208 A) teach the method of claim 10, further comprising preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file (see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed and that represent the act of prevention).

As per claim 12 Chen et al (5,832,208 A) teach the method of claim 10, further comprising preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application (see col.8, lines 7-15 where if the attachment or virus is not removed after the interception as outlined in claim 1 above, then attempt to cure the file being conducted and only in case of file repair that the agent may attachment may be re-attach to the file by the agent which means that if not cured or not removed the incoming file will not be forwarded by the agent).

As per claim 13 Chen et al (5,832,208 A) teach the method of claim 10, further comprising:

a) receiving a signal from said anti-virus application, said signal indicating

whether a virus was detected in the intercepted incoming file (see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5); and

b) communicating the signal to a user submitting the intercepted incoming file (see col.7, lines 60-65 where the alert may be transmitted to network node originated the infected attachment that corresponds to the user who submitted the virus in the first place).

As per claim 16 Chen et al (5,832,208 A) teach a program storage device readable by a machine (see fig.2, item 130 where the mail server corresponds to networked server that is a readable machine having storage device), tangibly embodying a program of instructions executable by the machine to perform a method for virus detection monitoring (see abstract where detection and removal of virus application in combination with server network and peripheral devices and interfaces corresponds to Applicant's virus detection monitoring system that monitors incoming files for virus), said method comprising:

a) intercepting the incoming files before the files are transferred to a file system of a server (see fig.2, item 110 where the agent check-in all incoming files; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to

the file system until the process of checking and re-attachment to the file are being processed); and

b) transferring the incoming files which are intercepted to an anti-virus application for virus detection and removal (see col.7, lines 48-67 where if virus detected then the infected attachment is being deleted).

As per claim 17 Chen et al (5,832,208 A) teach the program storage device of claim 16, said method further comprising preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file (see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed and that represent the act of prevention).

As per claim 18 Chen et al (5,832,208 A) teach the program storage device of claim 16, said method further comprising preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application (see col.8, lines 7-15 where if the attachment or virus is not removed after the interception as outlined in claim 1 above, then attempt to cure the file being conducted and only in case of file repair that the agent may attachment may be re-attach to the file by the agent which

means that if not cured or not removed the incoming file will not be forwarded by the agent).

As per claim 19 Chen et al (5,832,208 A) teach the program storage device of claim 16, said method further comprising:

a) receiving a signal from said anti-virus application, said signal indicating whether a virus was detected in the intercepted incoming file (see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5); and

b) communicating the signal to a user submitting the intercepted incoming file (see col.7, lines 60-65 where the alert may be transmitted to network node originated the infected attachment that corresponds to the user who submitted the virus in the first place).

As per claim 22 Chen et al (5,832,208 A) teach in a networked server (see fig.2, item 130 where the mail server corresponds to networked server) having a file system (see fig.2, item 140; col.7, lines 11-16 where the message system corresponds to applicant's file system) therein, a virus detection monitoring system (see abstract where detection and removal of virus application in combination with server network and peripheral devices and interfaces corresponds to Applicant's virus detection monitoring system that monitors incoming files for virus) comprising:

a) means for intercepting the incoming files before the incoming files are transferred to the file system of the server (see fig.2, item 110 where the agent corresponds to check-in interceptor as means for intercepting all incoming files; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed); and

b) means for transferring the incoming files which are intercepted to an anti-virus application for virus detection and removal (see col.7, lines 48-67 where if virus detected then the infected attachment is being deleted and the means for transfer if the agent 110 of fig.2).

As per claim 23 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 22, further comprising means for preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file (see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed and that represent the means of prevention).

As per claim 24 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 22, further comprising means for preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application (see col.8, lines 7-15 where if the attachment or virus is not removed after the interception as outlined in claim 1 above, then attempt to cure the file being conducted and only in case of file repair that the agent may attachment may be re-attach to the file by the agent which means that if not cured or not removed the incoming file will not be forwarded by the agent).

As per claim 25 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 22, further comprising:

a) means for receiving a signal from said anti-virus application, said signal indicating whether a virus was detected in the intercepted incoming file (see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5 as the means of detection of virus and alert as means of receiving the signal); and

b) means for communicating the signal to a user submitting the intercepted incoming file (see col.7, lines 60-65 where the alert may be transmitted to network node originated the infected attachment that corresponds to the user who submitted the virus in the first place).

Claim Rejections - 35 USC § 103

2. **Claims 6, 14, 20 and 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al (5,832,208 A) in view of Hodges et al (6, 269,456 B1).

As per claim 6 Chen et al (5,832,208 A) teach all limitation of the claim as applied to claim 1, above but do not explicitly disclose a "dat file updater and validater" coupled to the anti-virus application, said dat file updater and validater configured to periodically download updated virus data, validate the updated virus data after download, and update said anti-virus application with said updated virus data after validating said virus data. However Hodges et al (6, 269,456 B1) disclose a "dat file updater and validater" coupled to the anti-virus application, said dat file updater and validater configured to periodically download updated virus data, validate the updated virus data after download, and update said anti-virus application with said updated virus data after validating said virus data (see col.7, lines 1-12 where the file virus_signature.dat that corresponds to Applicant's dat file updater and validater configured to periodically such as monthly, or weekly, daily or even hourly update the dat file and validate the new update by integrating the new signature into the file virus_signature.dat by anti virus application manufacturer). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to

utilize Hodges et al's automated updating and upgrading of antivirus application system in Chen's anti virus detection system where every incoming file is being scanned by check in inceptor in order to provide the most up-to-date, or even up-to hour anti virus protection available.

As per claim 14 Chen et al (5,832,208 A) teach all limitation of method of claim 10 as applied above but do not explicitly disclose:

a) periodically downloading updated virus data;

b) validating the updated virus data; and

c) updating said anti-virus application with said updated virus data.

However Hodges et al (6, 269,456 B1) disclose periodically downloading updated virus data; validating the updated virus data; and updating said anti-virus application with said updated virus data (see col.7, lines 1-12 where the file virus_signature.dat that corresponds to Applicant's dat file updater and validater configured to periodically such as monthly, or weekly, daily or even hourly update the dat file and validate the new update by integrating the new signature into the file virus_signature.dat by anti virus application manufacturer). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hodges et al's automated updating and upgrading of antivirus application method in Chen's anti virus detection method where every incoming file is being scanned by check in inceptor in order to provide the most up-to-date, or even up-to hour anti virus protection available.

As per claim 20 Chen et al (5,832,208 A) teach all limitation of the program storage device of claim 16 as applied above but not explicitly disclose:

a) periodically downloading updated virus data;

b) validating the updated virus data; and

c) updating said anti-virus application with said updated virus data.

However Hodges et al (6, 269,456 B1) disclose the program storage device for downloading updated virus data according to a periodically downloading updated virus data; validating the updated virus data; and updating said anti-virus application with said updated virus data (see col.7, lines 1-12 where the file virus_signature.dat that corresponds to Applicant's dat file updater and validater configured to periodically such as monthly, or weekly, daily or even hourly update the dat file and validate the new update by integrating the new signature into the file virus_signature.dat by anti virus application manufacturer). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hodges et al's automated updating and upgrading of antivirus application virus detection program device for scanning incoming file by check in interceptor device in order to provide the most up-to-date, or even up-to hour anti virus protection available.

As per claim 26 Chen et al (5,832,208 A) Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 22, further comprising:

a) means for downloading updated virus data according to a schedule;

b) means for validating the updated virus data; and

c) means for updating said anti-virus application with said updated virus data.

However Hodges et al (6, 269,456 B1) disclose means for downloading updated virus data according to a schedule; means for validating the updated virus data; and means for updating said anti-virus application with said updated virus data (see col.7, lines 1-12 where the file virus_signature.dat that corresponds to Applicant's dat file updater and validater configured to periodically such as monthly, or weekly, daily or even hourly update the dat file and validate the new update by integrating the new signature into the file virus_signature.dat by anti virus application manufacturer). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hodges et al's automated updating and upgrading of antivirus application means in Chen's anti virus detection means where every incoming file is being scanned by check in inceptor means in order to provide the most up-to-date, or even up-to hour anti virus protection available.

3. **Claims 7, 15, 21 and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al (5,832,208 A) in view of McGrane (6,760,760 B1).

As per claims 7, 15, 21 and 27 Chen et al (5,832,208 A) teach all limitation of the claims including agent 11 of fig.2 that also corresponds to the virus detection monitoring system of claims 1, 10, 16 and 22, but do not explicitly disclose said

check-in interceptor inspects documents and files uploaded to an electronic document control system operating on the network server. However McGrane (6,760,760 B1) disclose uploaded of files to an electronic document control system operating on the network server (see fig.2-4 where the control system operating under the network server transfer uploaded data to the server; col.2, lines 61-63; col.4, lines 6-17 where it disclose a bi-directional communication and that the uploading of files are being send to the server where uploading may be in any direction). It also discloses more than one link between the server and the controller). It would have been obvious to one of ordinary skilled in the art to link MacGrane's file controller system where the uploaded file is stored to Chen's agent 11 of figure 2 that corresponds to check in interceptor in order to provide establish a pathway to one or more control systems to enable bi-directional transfer of uploaded data and files to be intercepted and scanned by Chen's anti virus interceptor agent.

4. **Claims 8 and 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al (5,832,208 A) in view of Tso et al (6,088,803 A).

As per claims 8 and 9 Chen et al (5,832,208 A) teach all limitation of the claim as applied in claim 1 above but do not disclose the interception of files comprising of uploaded commands and hypertext transfer protocol commands issued to the server. However Tso et al (6,088,803 A) disclose uploaded commands and hypertext transfer protocol commands issued to a server (see fig.5, item 36; col.7,

lines 13-23 where operation of read (uploading) and write (downloading) command for hypertext transfer protocol (http) is being processed where such file under that commands regardless of being uploaded or downloaded in any type of format such as html are subject to virus checker as disclosed on col.3, lines 2-4). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Tso et al's uploaded and HTTP commands in Chen's et al's anti-virus scanning file system in order to scan such internet downloaded/uploaded files for virus detection in order to prevent transmission of file and issuing an appropriate error warning message to client device or the server that holds the file.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available

through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

07/08/2005

AU2132